# Technical Whitepaper: Hybrid Passwordless Authentication in Banking

## 1. Executive Summary

### The Evolving Threat Landscape in Financial Services

The financial sector continues to face a rapidly evolving cyber threat landscape, with phishing attacks emerging as the most prevalent and damaging vector. In Poland, phishing incidents surged by 182% in 2021, accounting for 76% of all reported cyber incidents. Although 2021 marked a peak, the trend has remained troubling; in 2024, phishing still comprised 45% of all cyber attacks far outpacing threats like denial-of-service (16%). Notably, 60% of these phishing campaigns leveraged financial lures, specifically targeting bank customers. The persistent and adaptive nature of these attacks underscores the urgency for robust, phishing-resistant authentication methods in the banking sector.

### Project Goals: Security, Usability, and Fraud Reduction

BNP Paribas initiated this initiative in response to the increasing sophistication of cyber threats, particularly those exploiting the weaknesses of traditional password-based systems. The project's goals were threefold:

- **Enhance customer experience** by reducing friction in the authentication process.
- **Improve security** by deploying phishing-resistant mechanisms that limit the exposure of user credentials.
- **Reduce fraud and operational costs**, specifically by minimizing account lockouts previously averaging two per user annually and consuming 10–15 minutes per support incident.

This strategic investment in security and user experience aligns with the bank's broader vision of leading innovation in the Polish and global banking sectors.

### Strategy: A Hybrid Path to Passwordless Authentication

To achieve these objectives, BNP Paribas adopted a hybrid strategy that introduces passwordless authentication using passkeys, while maintaining support for legacy login methods during the transition period. Passkeys built on modern standards such as FIDO2/WebAuthn offer strong phishing resistance, seamless usability, and broad platform compatibility. However, their deployment in a banking context presents unique challenges due to the complexity of existing Identity and Access Management (IAM) systems.

This whitepaper explores the technical, strategic, and operational considerations of implementing a hybrid passwordless authentication approach in a regulated financial environment. It provides practical insights and lessons learned from BNP Paribas' journey, offering a model for other institutions navigating similar challenges.

## 2. Introduction

### Rethinking Authentication in the Modern Banking Era

For decades, password-based authentication has served as the default mechanism for securing online banking services. However, what was once considered a sufficient safeguard has become increasingly misaligned with both the expectations of modern digital users and the realities of today's threat landscape. Customers demand seamless, fast, and secure access to their accounts without the frustration of forgotten passwords, account lockouts, or clunky multi-step verifications. Meanwhile, attackers have evolved, routinely exploiting password weaknesses through phishing, credential stuffing, and social engineering.

### Unique Challenges in the Banking Sector

Financial institutions operate under stringent regulatory and security obligations, such as those defined by the revised Payment Services Directive (PSD2) and local supervisory frameworks. These mandates often require strong

customer authentication (SCA), secure data handling, and demonstrable resilience against fraud. At the same time, banks are disproportionately targeted by cybercriminals due to the high value of financial data and transactions.

Traditional authentication methods fall short in this environment. Passwords are not only inherently insecure but also expensive to support driving up costs through password resets, customer service load, and fraud mitigation. Additionally, the increasing prevalence of phishing attacks and credential reuse has made it clear that incremental improvements to password security are no longer sufficient.

### Purpose of This Whitepaper

This whitepaper presents a strategic and technical roadmap for implementing hybrid passwordless authentication in the BNP Paribas GOonline Biznes application. Developed from the joint initiative between BNP Paribas and Secfense, it showcases how Secfense's tools, expertise, and infrastructure enabled the seamless deployment of passkey-based login solutions. The paper offers a practical guide for institutions aiming to enhance security, ensure regulatory compliance, and deliver a frictionless user experience through a hybrid authentication approach.

By embracing a hybrid approach, introducing modern, phishing-resistant authentication mechanisms alongside existing login options, banks can modernize their security posture without disrupting their customer base. This paper outlines the rationale, challenges, design principles, and lessons learned from this transformation, providing a replicable model for other financial organizations navigating similar imperatives.

## 3. Terminology and Definitions

**Passwordless Authentication -** A method of authentication that does not require a password, using secure alternatives such as biometrics, passkeys, or cryptographic devices to verify identity.

**FIDO2 / WebAuthn -** An open standard for strong, passwordless authentication. FIDO2 includes the WebAuthn API, allowing web apps to authenticate users via device-bound credentials.

**Multi-Factor Authentication (MFA) -** A security process that requires users to present two or more independent credentials (e.g., something they know, have, or are) to verify identity.
**Credential Management -** The processes and technologies used to securely issue, store, update, and revoke authentication credentials across users and systems.
**Strong Customer Authentication (SCA) -** A regulatory requirement under PSD2 mandating authentication using at least two factors: knowledge, possession, and/or inherence.
**Passkeys -** Phishing-resistant, device-bound credentials that replace passwords. Passkeys are based on public-key cryptography and are compatible with FIDO2/WebAuthn standards.
**Load Balancer** - A network component that distributes incoming traffic across multiple servers or services to ensure high availability, scalability, and reliability of applications.
**SAML (Security Assertion Markup Language) -** An open standard that enables secure exchange of authentication and authorization data between identity providers and service providers.
**IdP (Identity Provider) -** A system or service that creates, maintains, and manages identity information and provides authentication services to relying applications.

## 4. Current Authentication Architecture

- Description of existing system (e.g., username + password, SMS OTP, hardware tokens).
- Overview of authentication flows in:
  - Mobile banking
  - Online banking
  - API channels

GOonline Biznes is one of BNP Paribas' most critical digital platforms, serving business clients and enabling secure, large-scale payment processing. Given the sensitivity and financial impact of the transactions handled through this system, the authentication process must strike a careful balance between robust security and operational usability.

Currently, users authenticate through a password-based login system, which is reinforced by multi-factor authentication (MFA). Depending on user preferences

and regulatory requirements, MFA can be fulfilled using mobile authentication and hardware tokens or one-time SMS codes.

While this architecture meets the requirements of Strong Customer Authentication (SCA) under PSD2, it still leaves room for improvement particularly in the context of modern phishing attacks, credential theft, and session hijacking. Despite MFA being in place, the password remains the weakest link, often targeted by attackers through phishing campaigns and credential stuffing.

Recognizing these risks, the bank initiated a strategic shift toward passwordless, phishing-resistant authentication. The objective was not only to enhance security but also to streamline the login experience for end users especially business clients operating in high-pressure, time-sensitive environments. This forms the foundation and rationale for the hybrid authentication approach described in the following sections.

## Organizational Context and Legacy Complexity

To fully understand the scope and ambition of BNP Paribas Bank Poland's authentication modernization efforts, it is essential to view them through the lens of the bank's broader technological evolution.

Over the years, the bank has undergone multiple mergers and acquisitions, each bringing a unique set of digital systems, authentication schemes, and infrastructure standards. While these strategic moves have expanded the bank's reach and capabilities, they have also significantly increased the complexity of the underlying IT landscape.

Every merger or acquisition introduced challenges such as:

- Integrating disparate IT environments
- Consolidating overlapping or redundant legacy systems
- Harmonizing diverse applications and services under a unified security and identity framework

These transitions have shaped the current state of the bank's infrastructure into a highly layered and interconnected ecosystem, a digital snowball that continues to grow in complexity. With interdependencies between legacy and modern components, implementing architectural changes, especially those touching critical systems like authentication requires:

- Careful planning
- Rigorous testing
- Resilient, modular solutions that can coexist with legacy components

This historical and architectural backdrop is crucial to understanding why a hybrid authentication strategy was chosen. Rather than pursuing a disruptive “rip-and-replace” approach, the bank needed a scalable, non-intrusive solution that could be gradually deployed across systems, clients, and platforms without sacrificing security or compliance at any stage.

## Legacy Login Flow in GOonline Biznes

BNP Paribas Bank Poland’s authentication architecture was designed with both security and discretion in mind. The system follows a layered approach where user interactions are being performed in the upper layer, while the majority of the authentication logic and data exchanges occur behind the scenes, fully shielded from the user and potential threat actors.

At the core of this model is a custom implementation of the SAML protocol, enabling federated identity verification between systems while limiting the exposure of sensitive user details.

### High-Level Flow (Pre-Hybrid Model)

1. **User Session Check**

   A user navigates to the GOonline Biznes application. The system first checks whether an active session exists.

2. **Redirection to Identity Provider (IdP)**

   If no session is found, the user is redirected to the centralized identity provider at login.bnpparibas.pl.

3. **User Authentication**

   At the IdP, the user provides:

   - A username and password

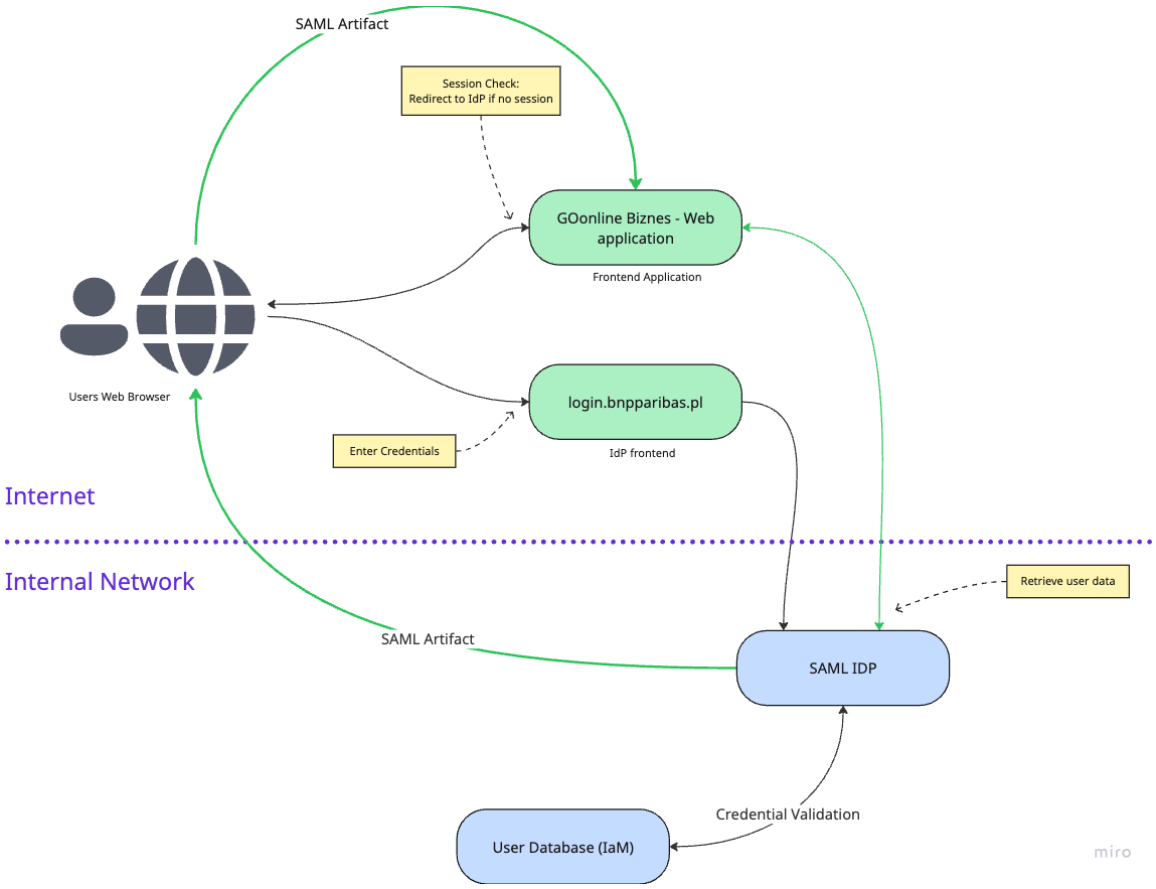
- A second factor (SMS code, hardware token, or software token)

4. **Decentralized Verification**
    - Password verification is handled internally by BNP Paribas systems.
    - Token validation is delegated to external components, depending on the type of token used.
    - The authentication process is orchestrated within BNP Paribas infrastructure, without exposing the internal mechanics to the user.
5. **SAML Artifact Transmission**

    Upon successful authentication, the IdP does not return full user details to the browser. Instead, it sends back a SAML artifact - a 32-character identifier - to the user's browser.
6. **Backend Artifact Resolution**
    - The GOonline Biznes application receives this artifact and, via a secure backend channel, resolves it by communicating directly with the IdP.
    - This exchange retrieves the user's identity and session information securely and invisibly to the user.
7. **Signature Verification**

    The GOonline Biznes system verifies the authenticity of the response using a public key, accepting only valid artifacts that are signed with a private key.

This architecture reflects a mature, security-first design philosophy. However, it also introduces complexity and rigidity, particularly in supporting modern authentication mechanisms such as passkeys, and adapting to phishing-resistant, passwordless login strategies.




# 5. Hybrid Authentication Strategy

## Design Constraints and Integration Strategy

Designing and deploying a passwordless authentication solution within BNP Paribas Bank Poland's enterprise environment required a deep understanding of the bank's architectural constraints and operational priorities. Given the critical nature of GOonline Biznes and the broader infrastructure, the approach had to be non-intrusive, secure, and fully backward-compatible.

### Key Constraints

Several foundational requirements shaped the design:

- **No changes to existing bank infrastructure**:

The architecture had to respect and operate within the bounds of current systems - including internal authentication mechanisms, MFA tools, and session management.

- **Preservation of legacy login options**:

  All previously available authentication methods (password + MFA, SMS codes, hardware/software tokens) had to remain fully functional and unaffected.

- **No modifications to GOonline Biznes**:

  The front-end application, due to its business-critical role and integration complexity, could not be altered at the code or infrastructure level.

- **No changes to the existing SAML Identity Provider (IdP)**:

  The centralized IdP system (login.bnpparibas.pl), which manages authentication flows across multiple services, also remained out of scope for code or structural changes.

- **Minimal service disruption**:

  The solution had to be deployed with minimal or zero downtime, ensuring continuity for customers and internal operations.

## Architectural Approach

To meet these stringent requirements, the design had to be:

- **Codeless**:

  No changes to source code or application logic in any existing system.

- **Agentless**:

  No software agents or additional modules installed on client devices or existing servers.

- **Interoperable via SAML**:

  The SAML protocol, already used for federated authentication between GOonline Biznes and the IdP, became the strategic integration point. By

leveraging SAML artifacts and intercepting the authentication flow at this layer, it became possible to introduce phishing-resistant passwordless authentication (e.g., passkeys) without disrupting the underlying architecture.

This strategy enabled the bank and its technology partner, Secfense, to embed a modern, passkey-enabled authentication layer into the existing login environment securely, seamlessly, and without compromising legacy operations or regulatory obligations.

## Content Adaptation: UI Integration Without Application Changes

One of the primary challenges in implementing passwordless authentication within the existing GOonline Biznes environment was the need to introduce graphical user interface (GUI) elements such as passkey registration prompts, login buttons, and account management panels without altering the application's codebase.

Given that no modifications were permitted within the GOonline Biznes front-end or back-end systems, traditional development approaches were off the table.

### Strategic Enabler: The Load Balancer

During the architectural assessment, the project team identified a central load balancer as a pivotal component in the bank's internal traffic routing infrastructure. This load balancer became the key enabler for integrating passwordless functionality in a non-invasive manner.

### Content Adaptation Technique

By leveraging the capabilities of the load balancer, the team was able to apply a technique known as content adaptation. This method allows dynamic injection or transformation of content in web traffic as it passes through the load balancer without touching the source code or underlying application logic.

Through content adaptation, the system now seamlessly injects passkey-related interface elements into the existing GOonline Biznes interface, including:

- Login buttons for passkey authentication

- Passkey registration workflows
- Authentication method management panels

These components are delivered on the fly, appearing natively within the application's UI, but are in fact externally managed and dynamically inserted.

This approach preserved the integrity of the legacy application while introducing a modern, passwordless experience fully aligned with security best practices and customer expectations.

## The Role of the Secfense Server in Passkey Integration

At the heart of the passwordless authentication infrastructure is the Secfense Server, a critical component that bridges modern authentication mechanisms with BNP Paribas' existing identity and access management (IAM) framework.

Although the user interface logic for the passwordless experience is delivered via the load balancer, the core orchestration, logic, and processing reside in the Secfense Server. It is the most pivotal component of the PASSKEYS ecosystem, operating in three primary roles:

### 1. Content Adaptation Engine

The Secfense Server serves the custom JavaScript front-end logic that enables dynamic insertion of passkey-related user interface elements into:

- The GOonline Biznes application, and
- The SAML Identity Provider (IdP) interface.

These front-end elements include login prompts, registration workflows, and credential management Uis - all injected without altering the existing application code.

### 2.FIDO2 Relying Party (RP)

As the FIDO2 server, the Secfense Server acts as a relying party, handling:

- Registration and binding of passkeys during onboarding
- Authentication validation during login

- Secure key storage and cryptographic operations in alignment with WebAuthn and FIDO2 standards

This makes the Secfense Server the gateway for all passwordless-related interactions and a key validator in the authentication process.

### 3. IAM API Consumer

The Secfense Server interfaces with BNP Paribas' IAM system via secured APIs. Through this integration, it is able to:

- Authenticate users after successful passkey verification
- Retrieve authorization data
- Validate permissions and grant access to GOonline Biznes accordingly

## Load Balancer Routing Rules for Passkeys

To route traffic efficiently between existing systems and the new passkeys layer, three custom rules were configured on the central load balancer, which sits in the middle of the BNP Paribas authentication infrastructure:

### Rule 1: JavaScript Injection

- Injects a JavaScript snippet into pages served by both the GOonline Biznes app and the IdP.
- This script loads the passkeys front-end logic dynamically, enabling content adaptation for UI elements related to login and passkey management.

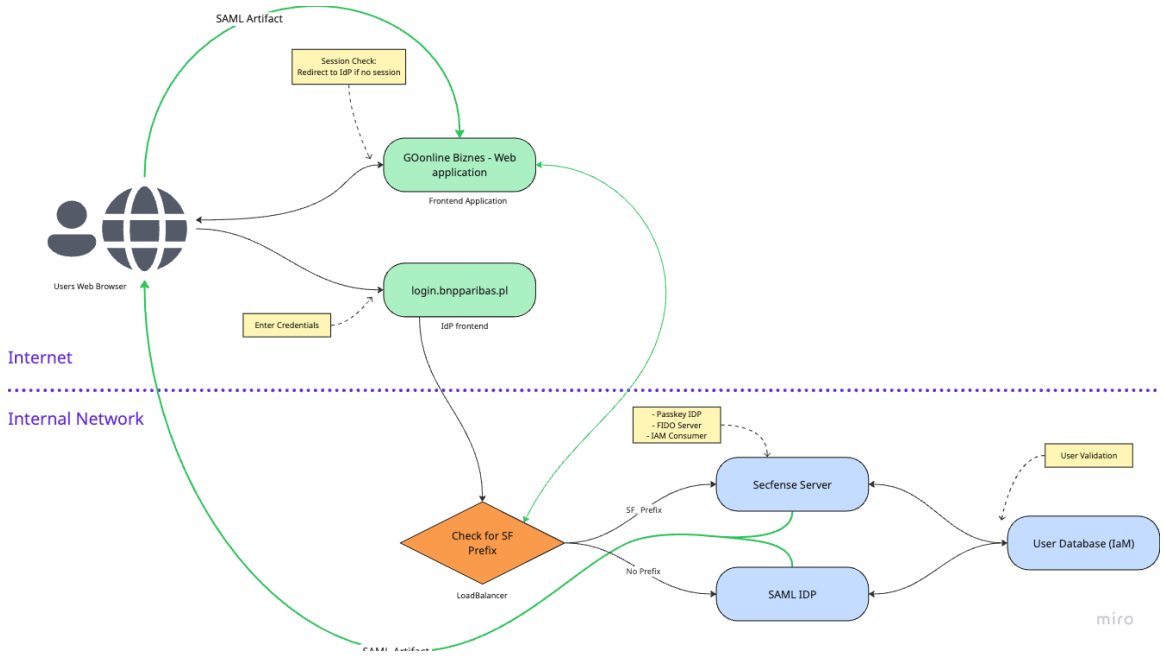
### Rule 2: Content-Based URI Routing

- UI elements related to passkey workflows (e.g., login, register) were designed to trigger requests to URIs containing the SF (Secfense Flag) prefix.
- This prefix allows the load balancer to identify traffic intended for the passkeys system and redirect it to the Secfense Server pool via content switching.

### Rule 3: SAML Artifact Interception

- All SAML artifacts involved in passwordless logic are also prefixed with SF.
- The load balancer uses this pattern to distinguish between legacy and passkeys flows, ensuring that passkeys artifacts are routed to the Secfense Server rather than to standard SAML endpoints.

This layered approach allowed the bank to introduce a modern, passkey-based authentication layer with zero impact on existing infrastructure, while maintaining clear separation between legacy and passkeys authentication logic. The result is a flexible, secure, and future-ready solution that integrates seamlessly into BNP Paribas Bank Poland's complex IT environment.




## Passkey Registration and Management

Among all the components of the passwordless solution, the passkey registration and management workflows were the most straightforward to implement thanks to the content-based routing mechanism already established using the SF (Secfense Flag) prefix.

## Seamless Redirection via Load Balancer

All user interactions related to passkey onboarding and management are initiated through UI elements injected dynamically into the existing GOonline Biznes and IdP interfaces. These elements, like the rest of the passkey interface, are served via JavaScript injection performed at the load balancer level, with the logic hosted on the Secfense Server.

When a user initiates one of these workflows (e.g., registering a new passkey or reviewing registered credentials), the associated requests are automatically routed to the Secfense Server. This is enabled by:

- Embedding the SF prefix in the URI of the request
- Intercepting that URI at the load balancer, which then redirects the traffic to the Secfense Server pool

This design ensures that:

- All registration and management processes are isolated from the legacy application logic
- The communication occurs exclusively between the user's browser and the Secfense Server
- No additional load or complexity is placed on existing systems

## Secure, User-Centric Flow

This approach guarantees a clean separation between the legacy authentication environment and the passwordless logic, while still providing a seamless experience within the familiar GOonline Biznes interface. All FIDO2-related operations such as credential creation, key storage, and credential revocation are handled directly by the Secfense Server acting as a FIDO2 Relying Party.

The result is a secure, user-transparent system that allows BNP Paribas business clients to register and manage passkeys with minimal friction without ever realizing that the underlying infrastructure has not been changed.

# 6. Compliance and Regulatory Considerations

## Compliance and Regulatory Considerations

### Passkeys Authentication Mechanism – PSD2 RTS Compliance Overview

The passkeys-based authentication mechanism implemented by BNP Paribas Bank Poland was audited for its alignment with the PSD2 Regulatory Technical Standards (RTS), particularly Chapters II and IV, which cover Strong Customer Authentication (SCA) and the confidentiality and integrity of credentials. The assessment confirmed a high degree of compliance, with minor recommendations for ongoing monitoring and user education due to reliance on third-party authentication technologies.

### Adherence to Strong Customer Authentication (SCA) Principles

The passkeys mechanism satisfies SCA by incorporating at least two of the following categories:

- **Knowledge** (e.g., a PIN)
- **Possession** (e.g., a device with a cryptographic key)
- **Inherence** (e.g., biometrics)

#### Authentication Code Generation

Each session begins with a unique challenge generated by the server, digitally signed by the user's private key stored securely on their device. This signature serves as a session-specific authentication code.

#### Confidentiality & Integrity

The digital signature reveals no information about the authentication elements (e.g., PIN, biometrics), maintaining the confidentiality of user data.

### Replay & Forgery Prevention

Each signature is uniquely tied to its challenge, preventing reuse and ensuring that only the legitimate device can generate valid responses.

### Failure Response

In case of a failed authentication, the system does not specify which element (e.g., PIN or biometrics) was incorrect, preventing brute-force reconnaissance.

### Session Management

While passkeys do not manage session length, the bank enforces a 5-minute inactivity timeout, meeting PSD2 requirements for online sessions.

## Article 5 – Dynamic Linking

Dynamic linking (specific to payment authorization) is not applicable to this implementation, as passkeys are only used for login and not for authorizing transactions in the GoOnline Biznes application.

## Article 6 – Requirements for "Knowledge" Elements

The solution supports third-party technologies such as Windows Hello, iCloud Keychain, Samsung Pass, Google Password Manager, and others. These technologies may rely on PINs or unlock patterns for local user verification:

- **Observation:** Some platforms allow weak or short PINs (e.g., "0000", "1111").
- **Bank Limitation:** The bank cannot enforce complexity rules for these PINs as they are governed by the device or operating system vendor.
- **Compliance Note:** This limitation does not violate PSD2 RTS, given the current use case (login only).

**Recommendation:** Launch user education campaigns promoting stronger security configurations and regularly monitor changes to third-party authentication practices.

## Article 7 – Requirements for “Possession” Elements

- **Private Key Security:** For locally stored passkeys, the cryptographic private key resides exclusively on the user’s device and becomes accessible only after local identity verification. For synchronized passkeys (e.g., via iCloud or Google Password Manager), the private key is securely copied between devices in encrypted form, and access to it still requires local user authentication.
- **Local Processing:** The key is never transmitted, reducing risk of compromise or duplication.

## Article 8 – Requirements for “Inherence” Elements

- **Biometric Use:** Biometrics (fingerprint, facial recognition, etc.) are supported via secure local methods like Windows Hello or hardware keys (e.g., YubiKey).
- **Secure Processing:** All biometrics are processed locally within trusted execution environments (e.g., Secure Enclave, TPM), ensuring they cannot be intercepted or exported.

## Article 9 – Independence of Elements

- **Separation by Design:** SCA elements (e.g., biometric and possession) are logically and technically independent.
- **Multi-functional Devices:** Devices that combine multiple roles (e.g., mobile phones) use secure local environments to prevent unauthorized access.
- **Tamper Resistance:** Secure environments resist modification; compromised software components are blocked through attestation mechanisms.

## Chapter IV – Confidentiality & Integrity of Authentication Data

- **Local Storage and Processing:** For locally stored passkeys, all sensitive data, including the private key, is generated, stored, and processed exclusively on the user’s device. For synchronized passkeys (e.g., via iCloud or Google Password Manager), the data is end-to-end encrypted

and securely transferred between devices, with local authentication still required to access the private key.

- **Encrypted Communication:** All traffic is protected with HTTPS. Only **public keys** are exchanged with the bank's servers.
- **Credential Masking:** Input fields for credentials are obscured at the OS level.
- **Encrypted Storage:** Credentials are never stored in plain text.
- **Hardware Isolation:** For locally stored passkeys, cryptographic material is protected within hardware-backed secure elements such as TPM, Secure Enclave, Android Keystore, or hardware tokens (e.g., YubiKey). For synchronized passkeys, protection relies on end-to-end encryption and the security mechanisms of the platform provider (e.g., Apple or Google), rather than dedicated hardware on the user's device.
- **Key Lifecycle Documentation:** The bank maintains full documentation of key management processes, including registration, invalidation, and renewal.

### Secure Credential Lifecycle

- **Secure Creation & Association:** Credentials are generated on the user's device and associated with their identity using SCA.
- **Remote Association:** During passkey registration, users must authenticate using SCA before associating a public key.
- **Delivery & Activation:** Credentials are never delivered remotely. Activation occurs locally after SCA.
- **Renewal:** If a device is replaced or lost, a new key is registered via the same secure process.
- **Deactivation & Invalidation:** Public key deactivation occurs via the bank interface; private keys are deleted on the user's device.

# 7. Integration and Deployment Plan

## Selective Deployment for Proof of Concept (Friends & Family Testing)

As the project approached the proof of concept (PoC) phase, the key objective was to introduce the new passkeys-based authentication functionality to a limited and controlled group of users, without impacting the broader production environment. This selective rollout, referred to internally as “friends and family testing”, required a method to discreetly activate the new features only for pre-approved individuals.

### The Challenge

The central challenge was to expose the passkeys-related interface components only to a selected group, without revealing them to the general user base. Several initial approaches were considered, each with distinct trade-offs:

- **Cookie-based Mechanism:** Technically viable, but raised the critical question of how to deliver the cookie only to the right users without relying on insecure practices.
- **Dedicated Access Links:** Considered and immediately dismissed. Sending test participants links via email would violate the bank’s strict security policies, as encouraging users to click on links in unsolicited emails could undermine anti-phishing education efforts and weaken overall user security posture.

### The Solution: Secfense Opt-In List and Cookie Injection

The team developed a secure and non-intrusive mechanism that combined internal data-driven targeting with dynamic UI control:

1. **Opt-In List in Secfense Database:**

   A dedicated list of user identifiers was created in the Secfense system, designating those eligible for the PoC. This predefined whitelist allowed precise control over who would experience the new authentication flow.

2. **Authentication-Time Evaluation:**

During the user authentication process, the system checks the SECFENSE opt-in list. If the user is on the list, the backend assigns a specific cookie to their session.

3. **Interface Logic Based on Cookie Presence:**

   The presence of this cookie then activates the visibility of passkeys-related HTML components, which are otherwise invisible to the rest of the user base. This behavior was achieved via the same front-end JavaScript logic injected by the Secfense server.

Outcome

This approach allowed the team to:

- Isolate the PoC experience to a known, secure group of testers.
- Avoid risky behaviors such as link-based distribution.
- Preserve the integrity of the production environment.
- Respect banking-grade security standards and UX principles.

The combination of cookies and backend user targeting via the SECFENSE database provided an elegant, secure, and reversible method for running real-world tests with minimal risk and maximum control.

# 8. Conclusion and Recommendations

The deployment of passwordless authentication mechanisms - specifically passkeys - at BNP Paribas Bank Poland demonstrates that moving beyond passwords is not a one-time switch, but a carefully orchestrated transition. It requires aligning security objectives with technical feasibility, regulatory compliance, and user expectations.

## Passwordless is a Transition, Not a Switch

Contrary to simplified narratives in the industry, eliminating passwords is not a binary decision. Especially in highly regulated environments like banking, passwordless adoption must coexist with legacy authentication during a defined transition phase. Systems need to support both new and old methods without compromising stability, compliance, or user trust.

This project illustrates how agentless and codeless technologies, such as the Secfense layer, can be leveraged to introduce passkeys without disrupting existing infrastructure. The dual-track model - where traditional methods remain available while passkeys are gradually introduced - ensures business continuity and operational resilience.

## Gradual Migration Is Key to Success

**The phased rollout approach - beginning with internal friends-and-family testing, followed by broader user opt-in - allowed the bank to gather real-world feedback, assess risk, and fine-tune the user experience. It also minimized the potential for support issues and ensured smoother onboarding for both users and administrators.**

**This gradual strategy is critical when working within complex, multi-layered IT environments, especially those that have evolved through mergers, acquisitions, and system consolidations. Introducing new authentication paradigms must be done incrementally, not disruptively.**

## Strategic Focus Areas for Banks

To successfully adopt passwordless technologies, banks should concentrate on the following areas:

- **Device Identity**:

  Strong authentication now begins with the device. The cryptographic material used for passkeys is tied to physical devices (e.g., smartphones, hardware keys), making the integrity and management of device identity a critical foundation of security.

- **User Experience (UX)**:

  The shift to passkeys should feel intuitive. Users expect authentication to be fast, simple, and unobtrusive. Any added friction increases the risk of resistance or support overhead. Seamless UI integration, transparent security flows, and clear guidance are essential.

- **Strong Fallback Mechanisms**:

  No authentication system is complete without a fallback plan. While passkeys provide high assurance, fallback methods must be equally

secure and well-managed. They should prevent lockouts while ensuring that recovery processes are resistant to fraud or social engineering.

## Final Thoughts

The success of this project lies not only in the technology but in the strategy and discipline behind its execution. BNP Paribas Bank Poland has demonstrated a model path forward for passwordless transformation, one that is realistic, secure, and scalable.

For other financial institutions considering similar initiatives, the key takeaway is this: passwordless is not about replacing one thing with another overnight it's about evolving toward a more secure, user-friendly, and future-ready authentication ecosystem.